

Державний вищий навчальний заклад  
«Донецький національний технічний університет»  
Кафедра Прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

\_\_\_\_\_ Леонід Бачурін

«\_\_\_\_\_» \_\_\_\_\_ 2024 р.

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**  
**ОНД 2.17 УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ**

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність (ості) \_\_\_\_\_ **125 Кібербезпека** \_\_\_\_\_

(шифр і назва спеціальності)

Освітня програма \_\_\_\_\_ **«Кібербезпека»** \_\_\_\_\_

(назва освітньої програми)

Мова навчання: українська

Луцьк – 2024

Робоча програма навчальної дисципліни «Управління інформаційною безпекою»

для здобувачів вищої освіти за спеціальністю 125 Кібербезпека

«25» грудня 2023 р – 8 с.

Розробник:

Маслова Н.О., к.т.н., доц., доц..каф.ПМІ

Робоча програма затверджена на засіданні кафедри прикладної математики та інформатики

Протокол №13 від 27.12.2023 р.

Завідувачка кафедри Прикладної математики та інформатики

\_\_\_\_\_  
(підпис)

( Маслова Н.О. )  
(прізвище та ініціали)

Схвалено науково-методичною комісією галузі знань 12 Інформаційні технології

Протокол №1 від 15.01.2024 р. \_\_\_\_\_ Голова \_\_\_\_\_  
(підпис)

(Башков Є.О.)  
(прізвище та ініціали)

## 1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	Обов'язкова	
Обсяг в кредитах ЄКТС	6	
Обсяг в годинах за навчальним планом, разом: в тому числі:	180	
лекції:	32	
практичні заняття:		
лабораторні заняття:	32	
семінари:		
самостійна робота:	116	
Форма підсумкового контролю	Екзамен	
Дисципліну викладають	Викладач Маслова Н.О. <a href="https://donntu.edu.ua/kitaer/pmi">https://donntu.edu.ua/kitaer/pmi</a> , <a href="mailto:nataliia.maslova@donntu.edu.ua">nataliia.maslova@donntu.edu.ua</a>	

**Передумови для вивчення дисципліни:** успішному вивченню дисципліни «Управління інформаційною безпекою» сприяє попереднє опанування такими дисциплінами, як: Основи інформаційної безпеки, Безпека програм та даних, Архітектура та проектування програмного забезпечення, Захист програмних реалізацій.

## 2. Мета вивчення навчальної дисципліни

**Метою** викладання дисципліни є оволодіння знаннями та вміннями, які утворюють теоретичний і практичний фундамент, необхідний для управління інформаційною безпекою й побудови систем захисту, проведення заходів які передують та супроводжують етапи забезпечення інформаційної безпеки на організаційному, адміністративному, технічному та інших.

### Компетентності:

- ФК04. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки
- ФК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

### Програмні результати навчання:

- ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових)
- ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем
- ПРН28 аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки;

- ПРН29. здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
- ПРН30. здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем
- ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків
- ПРН42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки
- ПРН44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами
- ПРН45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів
- ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах

### **3. Очікувані результати навчання**

Основними результатами опанування дисципліни “ **Управління інформаційною безпекою**” є:

- знання міжнародних та вітчизняними стандартами в галузі менеджменту інформаційної безпеки;
- володіння сучасними заходами управління інформаційною безпекою;
- опанування принципами розрахунку ризиків та їх значенням в системі управління безпекою;
- планувати менеджмент безпеки трудових ресурсів;
- знання особливостей формування політики інформаційної безпеки на рівні підприємства;
- навички з управління інцидентами інформаційної безпеки;
- опанування етапами підготовки до аудиту інформаційної безпеки та принципами його проведення

### **Внаслідок вивчення курсу студенти повинні вміти:**

- застосовувати міжнародні та вітчизняні стандарти;
- застосовувати методи та технології управління інформаційною безпекою;
- визначати загрози й вразливості об'єктів захисту, розраховувати ризики інформаційної безпеки;
- формувати політику інформаційної безпеки на рівні підприємства;
- організовувати заходи з реагування на надзвичайні ситуації (інциденти)
- проводити комплекс заходів підготовки до аудиту інформаційної безпеки;
- виконувати підготовчі дії з надання послуг у сфері інформаційної безпеки

### **4. Засоби діагностики результатів навчання**

Засобами оцінювання та методами демонстрування результатів навчання можуть бути:

- екзамен;
- лабораторні роботи;
- презентації результатів виконаних завдань та досліджень.

## 5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних занять) та підсумкового контролю. Максимальний бал, визначений схемою оцінювання, наведеною нижче, можливо отримати за умови своєчасного та правильного виконання завдань. За наявності помилок або при несвоєчасному виконанні оцінка знижується до 60% від максимальної.

Поточний контроль для очної/заочної форм навчання								Поточний контроль	Іспит	Максимальна сума балів
ЛР1	ЛР2	ЛР3	ЛР4	ЛР5	ЛР6	ЛР7	ЛР8			
5	5	5	5	5	5	5	5	40	60	100
3	3	3	3	3	3	3	3	24		

Примітки: 1) ЛР1, ЛР2 і т.д. лабораторні роботи;

2) У числівнику максимальний бал – при своєчасному та правильному виконанні, у знаменнику – мінімальний (при правильному, але несвоєчасному виконанні)

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

## 6. Програма навчальної дисципліни

### 6.1. Основні теми дисципліни

**Тема 1.** Основні напрямки розвитку менеджменту у сфері інформаційної безпеки

**Тема 2.** Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти

Лекція 1. Міжнародний стандарт ISO/IEC 27001 перелік захисних заходів та їх цілей

Лекція 2. Міжнародні стандарти в галузі інформаційної та /або кібербезпеки, Стандарти серії ISO/IEC 15408

Лекція 3. Стандартизація в сфері менеджменту. Регламенти ЄС в галузі кібербезпеки

Лекція 4. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки

**Тема 3.** Інформаційні технології в інформаційній та/або кібербезпеці

Лекція 5. Методи і засоби обробки інформації (алгоритми, мови)

Лекція 6. Алгоритми пошуку та сортування

**Тема 4.** Безпека інформаційно-комунікаційних систем

Лекція 7. Захист інформації, що обробляється та зберігається в ІКС

Лекція 8. Процедури ідентифікації, автентифікації, авторизації користувачів

**Тема 8.** Комплексні системи захисту інформації. Види забезпечення систем захисту  
Оцінка захищеності інформації в ІКС

Лекція 8. Проектування, створення, супровід КСЗІ

Лекція 9. Моделі загроз та моделі порушника

**Тема 9.** Управління ризиками в інформаційній та / або кібербезпеці.

Лекція 10. Ризики інформаційної безпеки

Лекція 11. Аналіз та оцінка ризику. Обробка ризику

**Тема 10.** Менеджмент інформаційної безпеки на рівні підприємства, основні напрямки і структура політики безпеки (ПІБ)

Лекція 12. Розробка політик ІБ під час забезпечення бізнес-процесів

Лекція 13. Дотримання політик інформаційної безпеки.

**Тема 11.** Організаційне забезпечення інформаційної безпеки міжнародних партнерів.

Лекція 14. Департамент інформаційної безпеки і робота з персоналом

**Тема 12.** Реагування на надзвичайні ситуації та управління кіберінцидентами

Лекція 15. Управління кіберінцидентами

**Тема 13.** Забезпечення безперервності бізнес-процесів

**Лекція 16.** Протоколювання та аудит.

### 6.2. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
1	ЛАБОРАТОРНА РОБОТА №1. Законодавча та нормативно-правова база в управлінні інформаційною безпекою	4	
2	ЛАБОРАТОРНА РОБОТА №2. Інформаційні технології в управлінні інформаційною безпекою	4	
3	ЛАБОРАТОРНА РОБОТА №3. Моделі безпеки	4	
4	ЛАБОРАТОРНА РОБОТА №4 Управління захистом інформації в ІКС	4	
5	ЛАБОРАТОРНА РОБОТА №5. Комплексні системи захисту інформації в управлінні інформаційною безпекою	4	
6	ЛАБОРАТОРНА РОБОТА №6 Адміністративний рівень управління інформаційною безпекою та управління кіберінцидентами (загрози, ризики)	4	
7	ЛАБОРАТОРНА РОБОТА №7. Розробка політик інформаційної безпеки	4	
8	ЛАБОРАТОРНА РОБОТА №8 Технічний рівень захисту інформації в управлінні безпекою	4	
	<b>Усього годин</b>	32	

### 6.3. Теми практичних занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Проведення практичних занять не передбачено		
2			
...	<b>Усього годин</b>		

#### 6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	
1	Загальні відомості з теорії інформації.	10	
2	Ідентифікація та автентифікація ресурсів СУІБ	10	
3	Методи надання доступу до інформації	10	
4	Методи контролю доступу до інформації	10	
5	Визначення критичних бізнес-процесів на прикладі банківських продуктів	10	
6	Поняття та особливості парольного захисту	10	
7	Вірусні атаки та антивірусний захист	10	
8	Методи захисту мереж банку	15	
9	Віддалений доступ до ресурсів мережі	15	
10	Хронологія розробки криптографічних алгоритмів	16	
	<b>Усього годин</b>	116	

#### 6.5. Індивідуальні та/або групові завдання

Не передбачено навчальним планом

### 7. Література

#### 7.1. Основна

1. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
2. Голев, Д.В. Методика оцінки інформаційної захищеності телекомунікацій: Навч. посіб. – Системи технічного захисту інформації, автоматизації її обробки. – Одеса, 2013. – 218 с.
3. Голев Д.В., Кільдишев В.Й., Кононович В.Г. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 1 – Комплекси засобів захисту інформації від НСД: Навч. посібник / За ред. чл.- кор. МАЗ В.Г. Кононовича.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С.176.
4. Д. В. Голев, О.Ю.Русяченко, Ю.В.Белова, Д.С.Гончарук Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 2 – Комплекси технічного захисту інформації Навч. посібник / За ред. чл.-кор. МАЗ В.Г. Кононовича.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 184.
5. Карачка А.Ф. Технології захисту інформації - Тернопіль, ТНЕУ, 2017. – 86с
6. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції. 2006. – 280с.
7. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.
8. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1,11 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.

#### 7.2. Допоміжна

1. Бакалінська, О. Правове забезпечення кібербезпеки в Україні / О. Бакалінська, О. Бакалинський // Підприємництво, господарство і право. 2019. № 9. – С. 100-108.

2. Корпоративна безпека: Практичний посібник. - КК Сідкон, 2018. - 276 .
3. Кібербезпека та ризики цифрової трансформації компаній. – Дакор, 2021. – 372
4. Ромака В. Системи менеджменту інформаційної безпеки Навчальний посібник / В.А. Ромака, В.Б. Дудикевич, Ю.Р. Гарасим, П.І. Гаранюк, І.О. Козлюк. Львів: Видавництво Львівської політехніки, 2012. 232 с.
5. Хорошко В.О. Проектування комплексних систем захисту інформації - Львів: - Львівська політехніка. -2020. – 320с.
6. Тарнавський Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки»; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с

### 7.3. Методична

1. Методичні вказівки для самостійної роботи з дисципліни «Основи інформаційної безпеки» для студентів спеціальності «Кібербезпека» денної форми навчання [Електронний ресурс] / уклад. Н.О.Маслова, О.І.Патрушева; . - Луцьк: ДонНТУ, 2019. – 49с.

код НТБ ДонНТУ: М625, режим доступу <http://ea.donntu.edu.ua/handle/123456789/30711>

### 7.4. Інформаційні ресурси

1. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти, [електронний ресурс], - режим доступу: <http://appj.wunu.edu.ua/index.php/appj/article/view/938>
2. Панченко В, менеджмент інформації безпеки комерційного підприємства [електронний ресурс], - режим доступу: [http://economics.kntu.kr.ua/pdf/3\(36\)/23.pdf](http://economics.kntu.kr.ua/pdf/3(36)/23.pdf)
3. Закон України «Про інформацію», [електронний ресурс], - режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12#text>
4. Закон України «Про доступ до публічної інформації», [електронний ресурс], - режим доступу: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
- Standart ISO/IEC-27001, [електронний ресурс], - режим доступу: <https://www.iso.org/ru/isoiec-27001-information-security.html>
6. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) [http://online.budstandart.com/ua/catalog/doc-page?id\\_doc=66910](http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910)